Long term strategy for a successful deployment of DNSSEC – on all levels

Workshop on Internet Technology Adoption and Transition (ITAT), December 4-6 2013.

Authors:

Anne-Marie Eklund Löwinder, Chief Information Security Officer, .SE, Trusted Community Representative appointed by ICANN for signing the root zone.

Patrik Wallström, CEO, OpenDNSSEC, project manager .SE

2013-08-13

Abstract

For the time being about 25 per cent of the .se zone file is signed using DNSSEC, a standard published as RFC 4033, RFC 4034 and RFC 4035 in March 2005. A number of our largest registrars are currently working to sign all their customer zones. All the largest ISPs in Sweden have turned on DNSSEC validation on the resolvers for their customers. A number of companies, organizations, municipalities and state agencies have turned on validation on their internal DNS. During our journey from 2005 we have ran into a number of interesting challenges and difficulties. From that we've learned a lot about deployment, operations and value of cooperation. This paper is pointing out some areas with remaining challenges and where we are lacking a long term strategy for the overall successful deployment of DNSSEC. Those areas are:

• Tools and Applications - Architectures, signing and key management practices, deployment guides, Risk Analysis of deployment. Who are in charge of defining what is needed to be defined?
• Educational Material - Material that explains the value and benefit of DNSSEC, awareness rising, staff training, guidelines and policy framework.
• Incentives - A push for organizations to take action or incentives to influence their decision. What and how?
• Future development – Given DNSSEC, DNS might be used for several other purposes, especially distribution of different information security credentials such as keys, identities, policy identifiers and more. DANE is a perfect example of the possibility to make use of DNS in such a manner. How can we explain the beneficial outcome of such an approach?

The .SE journey towards full deployment of DNSSEC

A certain number of TLDs have already signed their zones with DNSSEC, .SE being the first to deploy in 2005. What has been a little bit special for Europe is that there are a small number of TLDs that have been quite doubtful towards DNSSEC, some of them of significant size. Lately they have been more or less forced to accept the deployment of DNSSEC, though still not convinced of the value or benefits.

Given the current deployment status of DNSSEC, we would like to present and discuss our experiences from the registry working with hosting providers, registrars and registrants in order to convince them to implement DNSSEC.

Why is DNSSEC not there already?

Or, you may ask yourself: Why is DNSSEC still controversial among certain groups?
We would like to address possible remaining challenges to the deployment. The different areas that we would like to address are:

- Tools and Applications - Architectures, signing and key management practices, deployment guides, Risk Analysis of deployment. Who are in charge of defining what is needed to be defined?
- Educational Material - Material that explains the value and benefit of DNSSEC, awareness rising, staff training, guidelines and policy framework.
- Incentives - A push for organizations to take action or incentives to influence their decision. What and how?
- Future development – Given DNSSEC, DNS might be used for several other purposes, especially distribution of different information security credentials such as keys, identities, policy identifiers and more. DANE is a perfect example of the possibility to make use of DNS in such a manner. How can we explain the beneficial outcome of such an approach?

Long term strategy for a successful deployment of DNSSEC – on all levels

As a TLD you need to work on all different fronts to get things move forward. It doesn't matter much if your TLD zone file is signed if there are no first-level domains that are signed, and even more so, it doesn't matter much if the first-level domains are signed if no one cares to validate the signatures and take the proper action if the validation fails.

You have to work with different partners and stakeholders:

- Hosting Providers
- DNS Providers
- Other TLDs
- Registrars
- Registrants
- Interest groups

In a number of different ways:

- Financial
- Legal
- Technical

Financial incentives

We used to believe that there is more to do in this area but to just "encourage" the registrars and large DNS hosting providers to sign their customer zones. Other stakeholders to take into consideration are the ISPs as well as the registrants. For instance, in Sweden we decided to support the name service provider that manages different governmental agencies DNS to embrace DNSSEC, tempting them with one hundred freely available consultant hours from the most skilled DNSSEC consultants available by that time (3-4 years ago). Didn't work very well.

One activity worth mentioning is that we encouraged The Swedish Civil Contingencies Agency, MSB, to grant funds under appropriation bill 2:4 Crisis Contingencies, which can be applied for by designated government agencies. For 2012, MSB has prioritized reinforcement measures to facilitate secure online address searches, which are conducted via the DNS domain-name system. Among other remarks, MSB says that "it is vital that domains for public web sites are signed using DNSSEC." This activity will be prolonged to cover 2014 as well.

Municipalities can apply for funds through the County Administrative Boards. Municipalities throughout the country have been sending in their applications. We are assisting in all possible ways. In partnership with MSB, our regulator, the Swedish Post and Telecom Agency, PTS, and the Swedish Association of Local Authorities and Regions, SALAR, .SE has developed a package solution, which includes application forms that municipalities can use to apply for funds. Municipalities are able to get expert help with any questions they have, advice about knowledgeable consultants to get support from, training courses as well as other material, like guidelines with definition of requirements to get a high quality service.

Now, we are back to working with registrars, giving them a kickback for every signed domain, counted every six month. It seems to be the best way to move forward. We are of the opinion that DNSSEC is a way to strengthen the DNS infrastructure, and that a registrar don't need the registrants permission to sign domains. You may though give them the opportunity to opt-out, not that we think they will, it simply seems to be a reasonable way to make DNSSEC deployment happen without getting into too much trouble with the contractual part.

Tools

We believe that DNSSEC are still lacking tools for large name server operators (typically a registrar) to support the signing of large numbers of domains. Better and more suited tools still needs to be developed.

.SE is one of the founders of the OpenDNSSEC project, bringing our experience with early deployment into the project. OpenDNSSEC is now used by many TLDs.

There is a strong need of APIs for communication with a parent zone. Today there is no standardized mean to distribute keys for publishing from child to parent. That sort of interface needs to be developed and implemented, and work on standardization is going on in the IETF dnsop working group.

We would like to point out that .SE supported an implementation of DKIM validation with DNSSEC back in 2008. DKIM Milter already supports DNSSEC. It is named OpenDKIM. You may find a report on:
http://liu.diva-portal.org/smash/record.jsf?pid=diva2:128399

Monitoring

Inasmuch DNSSEC increases the requirements on quality for both DNS and zone management, tools need to be developed that support the registrant to check DNSSEC for their own domains as well as for the parent zone in order to check on all the delegated zones for DNS and DNSSEC quality.

In .SE we have developed both dnscheck and dnssec-analysis, which are both available as open source. An activity worth mentioning is for instance http://kommunermeddnssec.se where the deployment of DNSSEC (and IPv6) in Swedish municipalities is shown over time. Visualizing the deployment gives you a very quick overview of the current status.

Third party monitoring is an important addition to in house monitoring. One example from Sweden is http://www.dnssecandipv6.se/ where you may find the status based on different branches. It uses the .SE tool DNSCheck as an engine. As you can see, this is made not only for Swedish agencies, municipalities and companies, but also for U.S. Texas counties.

Specification of requirements on DNSSEC on different levels

We lack specified requirements on registries, registrars, name serving operators and registrants. Each of them has a significant role to play. A specification on what requirement to put on what stakeholder respectively is essential and makes it easier to understand the role and responsibilities for the different actors.

We have recently published a guideline of recommended requirements to consider when deploying DNSSEC within your organization or asking a third-party to do so on your behalf. The main target is the municipalities, but the guidelines may of course be used of any SME or similar entity. The guideline is only available in Swedish.

Authoritative Servers and Resolvers

There are a number of different instances of authoritative name servers as well as resolvers. We would appreciate an overview where a description of each and everyone is available, and where they are tested and compared with performance and other parameters important to get a reliable DNSSEC service.
Stub resolvers and clients need to fully support DNSSEC validation in order to make use of TLSA validation on web and mail services. However, CPEs are still not fully capable of handling the "new" DNS extensions and the larger packets. More work is needed in examining the deployment of new technology at all types of edges in the network.

DNSSEC capable Mobile Operating Systems

NLNetLabs have developed an IOS version of libUnbound. So, it is possible already to build applications within IOS and with DNSSEC validation support. That area may be improved by covering more name server software and more mobile platforms.

Managed DNS Services

It is of our opinion managed DNS services may add complexity and third party dependencies that one need to take into consideration when choosing the way forward on how to deploy DNSSEC. There is a significant risk that people overestimate the value of that kind of services. It would be nice to have a risk analysis spent on the different situations that might take place, choosing a managed DNS service. Specification of requirements on signing by a third party would be equally valuable.

DNSSEC Hardware

In 2010 .SE contracted a consultant firm to perform a review of available HSMs and how they work together with DNSSEC and OpenDNSSEC using PKCS#11. That review is probably of some value to a broader audience and should probably be repeated and updated.
http://www.opendnssec.org/wp-content/uploads/2011/01/A-Review-of-Hardware-Security-Modules-Fall-2010.pdf

Documents & Regulations - Best Practices, Tutorials and Manuals

.SE has been working to define RFC 6841, A Framework for DNSSEC Policy and Practice Statement that was accepted in January 2013. Its use is wide spread already by some number of TLDs, the root included, and by the applicants of new gTLDs, since DNSSEC is mandatory for them, and the requirement in the Applicant Guide Book is to use that framework as a template to describe the DPS.

The document presents a framework to assist writers of DNSSEC Policies and DNSSEC Practice Statements, such as Domain Managers and Zone Operators on both the top-level and secondary level, who are managing and operating a DNS zone with Security Extensions (DNSSEC) implemented. In particular, the framework provides a comprehensive list of topics that should be considered for inclusion into a DNSSEC Policy definition and Practice Statement, and to reflect the actual environment.

It is also worth mentioning the revised version of RFC4641, namely RFC6781, where the practice for operating the DNS with security extensions (DNSSEC) is in focus. The target audience is zone administrators deploying DNSSEC.

Thirdly, there is a draft that describes a set of common problems and possible recovery methods for DNSSEC when there is a DS published in the parent zone which does no longer match any DNSKEY in the child zone. As DNSSEC validators are becoming widely deployed, this will have serious effect on the availability of the zone, and the need for a quick recovery is strongly needed.
https://github.com/yyoneya/dnssec-kskro-frp
http://tools.ietf.org/html/draft-yoneya-dnssec-kskro-failure-recovery-00

Political

There are some very critical parameters in regard to DNSSEC that is important to consider in deployment, management and operations. In .SE we regularly perform studies within our program "The eco system of the Internet". The aim is to monitor the quality of the Internet's infrastructure in Sweden by compiling and analyzing facts, to disseminate the results from the surveys, and to use advice and recommendations to contribute to ensuring that the infrastructure functions well and has a high level of accessibility. The latest contribution to this range of studies is about DNS and DNSSEC. You may read about our findings in the report. Some of them are quite interesting and shows the need of definitions different DNSSEC related parameters. For instance, one common administrative problem is that many DNSSEC signed domains appear to be lacking a link between the period of validity for the zone and the period of validity for their signing keys – in other words, the value in the field *SOA Expire* often lacks a link to *RRSIG expiration* time. This may result in problems with reachability since you run the risk of keys becoming invalid without warning. Another problem is domains that have signature lifetimes that are unusually long or too short. We would definitely encourage general improvements in that area.

Something that we've learned over time is the value of specifying a Key and Signing Policy (KASP) where you may define the parameters that you need to consider, separating the policy on DNSSEC from the process of signing with DNSSEC. A KASP describes the issues surrounding the timing of events in the rolling of a key in a DNSSEC-secured zone. It presents timelines for the key rollover and explicitly identifies the relationships between the various parameters affecting the process. To define a KASP and to refer to it in a DPS solves the problem of changing the DPS every single time when you need to change parameters in the KASP.

Other DNS Rulemakers

As mentioned before The Swedish Civil Contingencies Agency, MSB, are granting funds under appropriation bill 2:4 Crisis Contingencies, which can be applied for by designated government agencies. We run a joint project, and the last result is that they will prolong the application period with yet another year. The first year (2012) 86 municipalities (out of 290) were granted funding.

CENTR is the European country code TLD not-for-profit organization dedicated to supporting the interest of country code TLD managers. The objectives of CENTR are to promote and participate in the development of high standards and best practices among ccTLD Registries. In that capability CENTR is very strongly promoting DNSSEC by arranging workshops, benchmarking and statistics.

Deployment and Operations

Validation is an important area to develop, in relation to end-system validation and validating applications. For instance, validation in itself doesn't require that all zones are signed. Something that would be interesting to elaborate more is the difference between "strict" and "permissive" state, and the actual value of DNSSEC if people choose to use permissive state for validation. Moreover, we would like to advice against the use of permissive state.

Validation

We would like to refer to the earlier mentioned monitoring system. Even though it is difficult to monitor validation it is nonetheless important to measure quality and stability in a top level domain while deploying and trying to understand DNSSEC.

All the large Swedish ISPs have embraced DNSSEC. One of the benefits of living in a small country is that everyone knows each other and is willing to cooperate. For instance, within .SE we have a DNS reference group consisting of ISPs, registrars, the registry and a number of other DNSSEC skilled individuals that discuss difficulties and exchange experiences. The reference group meets regularly exchanging experiences with DNS and DNSSEC, and also discusses new trends in the area. That is a very good way in stepping forward. All the single actors don't need to be barking up the wrong tree.

Firewalls and routers

We would like to elaborate more on the harm that firewalls and routers may cause DNSSEC due to the fact that they are not properly designed for DNSSEC. To put it bluntly there are still firewalls that consider DNSSEC packets to be harmful or too large, and therefore throw them away, which of cause effects the validation experience for end users and applications. There was a very interesting article on this subject in Internet Protocol Journal, Volume 13, No. 2. Note especially footnote 2 and 3 respectively.

Another interesting work is taking place within the IETF where the Senior Researcher at Nominet, Mr. Ray Bellis is co-chairing the Homenet wg.

DNSSEC Based Applications

There are a number of DNSSEC based applications that already exists. We specifically want to mention SSH with DNSSEC, http://www.ietf.org/rfc/rfc4255.txt, which is using DNS to securely publish Secure Shell (SSH) Key Fingerprints.

DKIM is already there as mentioned before. That needs to be further developed/improved, for instance, the error codes for DNSSEC validation errors is still lacking. The DMARC wg is working on higher-level use of DKIM and SPF.

Finally, we are putting a lot of expectations on the outcome from the DANE working group, a wider deployment of clients making use of the TLSA records published in DNS.

Next Steps for the Deployment of DNSSEC

We have mentioned earlier in this document that tools to sign large numbers of zones is strongly needed.

About checking signed zones, the tool DNSCheck developed by .SE is one tool that is already there for checking by both the registrant and the party that is signing the zone capable to both verify and monitor DNSSEC. One feature in DNSCheck is that you may check the quality even before the zone is delegated (undelegated check).

What should be added to the todo-list: Encourage the deployment of TLSA for safe validation of certificate (DANE).

Products & Services

The massive signing who has taken place in .cz and .de (not to mention in .se and the latest addition .nl) is the result of a close work together with the registrars and name server operators, not only by the TLDs themselves.

DANE

The possibility to use DNS-Based Authentication of Named Entities (DANE) to improve the security for an identity federation is a clear case of DNSSEC benefits. Improvements can be made on how identity federations handle their own metadata and trust other entities metadata. Now, since DANE with TLS/TLSA has become an RFC it certainly can be used to improve the initial trust bonding, adding a particularly important piece of a trust architecture model, in a world where we realize more and more that you cannot trust anything that you aren’t in control of.